CLAIMS

1. A method of encrypting binary data using block encryption and a private key, the method comprising:

generating a series of coding transforms using said private key, said series of coding transforms being generated in a repeatable manner;

each coding transform of the series adapted to modify elements within a block of said binary data to be encrypted; and

encrypting blocks of said binary data by selectively applying said coding transforms.

2. A method of encrypting binary data according to claim 1, wherein a different coding transform of said series is used to encrypt each said block.

3. A method of encrypting binary data according to claim 2, wherein sequentially generated coding transforms of said series are used to encrypt sequential blocks containing said binary data.

4. A method of encrypting binary data according to claim 1, wherein each coding transform of said series is adapted to transpose elements within the block of binary data to be encrypted.

5. A method of encrypting binary data according to claim 1, wherein each coding transform of said series is adapted to selectively invert ones of said elements within the block of binary data to be encrypted.

6. A method of encrypting binary data according to claim 1, wherein each coding transform of said series is adapted to transpose elements within a block of binary data to be encrypted and to selectively invert ones of those elements.

7. A method of encrypting binary data according to claim 6, wherein each coding transform of said series is generated as one sub-transform for achieving the transposition function and another sub-transform for achieving the inversion function, and wherein said sub-transforms are applied in any order in the encrypting step.

8. A method of encrypting binary data according to claim 1, wherein said series of coding transforms is generated in a pseudo-random manner.

9. Encryption apparatus for performing the method of claim 1, the apparatus comprising:

an input buffer for receiving plain blocks of binary data to be encrypted;

an input register for receiving said private key;

an arithmetic unit for generating a series of control outputs, corresponding to said series of coding transforms, using said private key;

logic circuitry, responsive to said series of control outputs, for converting input plain blocks of binary data to encrypted blocks of binary data in accordance with said series of coding transforms; and

an output buffer for outputting said encrypted blocks of binary data.

10. A computer program product for encrypting binary data using block encryption and a private key, the product comprising program code constituting a set of instructions for performing the method of claim 1 when the program embodied in said product is executed on a processor having a computing function, a computer, or a computer network.